20∗) (GAP, Continuation of problem 14) In this problem we are working modulo 3. Consider the ring $R$ of 9 elements which you obtained in problem 14 by considering polynomials modulo $f(x) = x^2 - 2$ and modulo 3.

a) Show that the polynomials of degree zero create a subring. We can identify this subring with $\mathbb{Z}_3$ (which are the integers modulo 3).

b) Show that the equation $y^2 + 1 = 0$ has no solution in $\mathbb{Z}_3$.

c) Show that the equation $y^2 + 1 = 0$ has a solution in $R$. (We therefore could consider $R$ as $\mathbb{Z}_3[i]$.)

d) Show that every nonzero element of $R$ has a multiplicative inverse and conclude that $R$ is a field.

e) Now suppose we repeat the same construction, but with the polynomial $x^2 - 1 = (x + 1)(x - 1)$. Do we get a field as well? Explain.

21) Show that $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ is a field.

22) Let $R$ be a ring with 1 (unity) and $a \in R$ a unit (i.e. an invertible element). Show that the inverse of $a$ must be unique.

23) Let $R = \mathbb{Z}_{40}$. Determine the units and the zero divisors of $R$.

24∗) Let $R$ be a ring of characteristic $p$. Show that for all $a, b \in R$ we have that $(a + b)^p = a^p + b^p$.

(Hint: Binomial Theorem – show that $\binom{p}{k} \equiv 0 \pmod{p}$ for $2 \leq k \leq p - 1$.)

25) Let $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ and let $S = \{a + bi \mid b \text{ even}\}$. Show that $S$ is a subring of $\mathbb{Z}[i]$ but not an ideal.

26) Determine all subrings, ideals and principal ideals of $\mathbb{Z}_{12}$.

27) Let $R$ be a field. Show that $\{0\}$ and $R$ are the only ideals of $R$.

28) Let $R = \mathbb{Q}[x]$ and let $A = \{f \in R \mid f(0) = 0\}$ and $B = \{f \in R \mid f(0) = 1\}$.

a) Show that $A \triangleleft R$.

b) Is $B \triangleleft R$?

c) Show that $A$ is a principal ideal of $R$ and find a generator of $A$. (Hint: You need to find a polynomial $p(x)$ such that $p(x) \mid f(x)$ whenever $f(0) = 0$.)

Problems marked with a $∗$ are bonus problems for extra credit.
Sample Midterm Problems

The first midterm will be on September 30. You need only pencil and eraser, you may bring an ordinary pocket calculator (but not a laptop, PDA, mobile phone or similar), though you probably will not need it.
This is a set of problems which are (or are similar to) previous semesters midterm problems. The actual midterm problems will be chosen to be similar to these or to homework problems (though the total number of midterm problems will be smaller).

1) Find an integer \(x\) such that \(5x + 7 \mod 41 = 3\).

2) Let \(S = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}\).
   a) Show that \(S\) is a subring of \(\mathbb{C}\).
   b) Show that \(S\) is a field.

3) Let \(R = \mathbb{Q}[x]\) and let \(A = \{f \in R \mid f(1) = f(2) = 0\}\). Show that \(A\) is an ideal in \(R\).

4) Let \(R = \mathbb{Z}_{12}\). Determine the units and the zero divisors of \(R\).

5) Let \(R\) be an integral domain, such that \(0\) and \(R\) are the only ideals of \(R\). Show that \(R\) is a field.
   (Hint: Consider the principal ideal \((a)\) for \(0 \neq a \in R\).

6) Let \(R = \mathbb{Z}\) and \(I = \langle 15, 21 \rangle_R\). Is \(35 \in I\)? Explain!

7) Prove (anew, we already had this proof in the lecture) that in an integral domain \(ab = ac\) implies \(b = c\) for \(a \neq 0\).

8) Let \(R = \{0, 2, 4, 6, 8, \ldots, 28\}\) with arithmetic modulo 30.
   a) Show that 16 is the identity element of \(R\). (Hint: You must show \(2 \cdot a \cdot 16 \mod 30 = 2 \cdot a\), use that \(2 \cdot 16 \mod 30 = 2\).)
   b) Show that if \(a \in R\) such that \(\gcd(a, 30) = 2\) then \(a\) is a unit.
   c) Is \(R\) an integral domain?

8) Construct the multiplication table for the field with 4 elements by using polynomial arithmetic modulo 2 and modulo \(x^2 + x + 1\).